AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

land or in a Federally operated (or contracted) facility and involve the professions/activities performed by persons specified in the Crime Control Act of 1990, including, but not limited to, physicians, nurses, dentists, health care practitioners, optometrists, psychologists, emergency medical technicians, alcohol or drug treatment personnel, child care workers and administrators, emergency medical technicians and ambulance drivers.

(c) The Contracting Officer shall insert the clause in *352.237–72*, Crime Control Act—Requirement for Background Checks, in solicitations, contracts, and orders that involve providing child care services to children under the age of 18, including social services, health and mental health care, child- (day) care, education (whether or not directly involved in teaching), and rehabilitative programs covered under the Crime Control Act of 1990 (Act).

PART 339—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 339.1—General

Sec.
339.101 Policy.

Subpart 339.2—Electronic and Information Technology

339.201 Clarification.
339.201–70 Required provision and contract clause.
339.203 Approval of exceptions.

Subpart 339.70—Use of General Services Administration Blanket Purchase Agreements for Independent Risk Analysis Services

339.7000 Policy.
339.7001 Request for approval to make an award to other than a GSA BPA holder.
339.7002 Notice of intended award.

Subpart 339.71—Information Security Management

339.7100 Definitions.
339.7101 Policy.
339.7102 Applicability.
339.7103 Solicitation and contract clause.

AUTHORITY: 5 U.S.C. 301; 40 U.S.C. 486(c).

SOURCE: 74 FR 62398, Nov. 27, 2009, unless otherwise noted.

Subpart 339.1—General

339.101 Policy.

(d)(1) The Contracting Officer shall insert the clause in *352.239–70*, Standard for Security Configurations, in solicitations, contracts, and orders that involve the operation or acquisition of an information technology system (for definition of the latter term, *see http://www.hhs.gov/ocio/policy*.)

An HHS information security policy waiver, the template for which is available at: *http://intranet.hhs.gov/infosec/policies_memos.html*, must be approved in order to deviate from HHS OCIO Standard 2009–0001.001S, HHS Standard for Security Configurations Language in HHS Contracts, dated January 30, 2009. A copy of the approved waiver shall be forwarded to the Contracting Officer who, in turn, shall request a comparable deviation for the clause in *352.239–70*.

(2) The Contracting Officer shall insert the clause in *352.239–71*, Standard for Encryption Language, in solicitations, contracts, and orders that involve the acquisition or lease of, or the requirement to use, desktop or laptop computers, mobile devices, or portable media to store or process HHS sensitive information that the Project Officer categorizes as moderate or high under Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004. An HHS information security policy waiver, the template for which is available at: *http://intranet.hhs.gov/infosec/policies_memos.html*, must be approved in order to deviate from HHS OCIO Standard 2009–0002.001S, HHS Standard for Encryption Language in HHS Contracts, dated January 30, 2009. A copy of the approved waiver shall be forwarded to the Contracting Officer who, in turn, shall request a comparable deviation for the clause in *352.239–71*.

Subpart 339.2—Electronic and Information Technology

339.201 Clarification.

FAR Subpart 39.2, Electronic and Information Technology, requires Federal

agencies to ensure that, when acquiring EIT, Federal employees with disabilities and members of the public with disabilities have access to and use of information and data that is comparable to individuals without disabilities. This EIT access requirement does not apply to a contractor's internal workplaces. EIT that is neither used nor accessed by Federal employees or members of the public is not subject to the Access Board accessibility standards. Contractors in their professional capacity are not members of the public for purposes of Section 508.

339.201–70 Required provision and contract clause.

(a) The Contracting Officer shall insert the provision in *352.239–73(a)*, Electronic and Information Technology Accessibility, in solicitations valued at more than the micro-purchase threshold that involve the development, acquisition, maintenance, or use of EIT products and services subject to Section 508 of the Rehabilitation Act of 1973, as amended, including EIT deliverables such as electronic documents and reports. (NOTE: Exceptions to this requirement can be found in *FAR 39.204*.) After approval of the Section 508 Official or designee, the Contracting Officer may waive the requirement for offerors to provide an HHS Section 508 Product Assessment Template, if Section 508 EIT conformance can be determined conclusively through other less formal methods. The Contracting Officer shall document in the award file any waiver for submission of the Product Assessment Template. The approval of a waiver by the Section 508 Official does not, however, eliminate the requirement for product assessment against Section 508 accessibility standards.

(b) The Contracting Officer shall insert the clause in *352.239–73(b)*, Electronic and Information Technology Accessibility, in contracts and orders that involve the development, acquisition, maintenance, or use of EIT products and services, including EIT deliverables such as electronic documents and reports, subject to Section 508 of the Rehabilitation Act of 1973, as amended, unless the EIT products and services are incidental to the project. (NOTE: Other exceptions to this requirement can be found at *FAR 39.204*.)

(c) When acquiring EIT products and services subject to Section 508 of the Rehabilitation Act of 1973, as amended, in the following circumstances, the Contracting Officer shall insert the paragraph in *352.239–73(c)*, Schedule for Contractor Submission of Section 508 Annual Report, which requires a contractor to provide an HHS Section 508 Annual Report, at the end of the clause in *352.239–73(b)* and cite the schedule for report submission, where indicated:

(1) New multiple-year contracts.

(2) Existing multiple-year contracts, with a performance period of 1 year or more remaining as of January 16, 2008 (the effective date of HHS' interim acquisition guidance).

(3) New multiple-year task and delivery orders exceeding $100,000 awarded under IDIQ or FSS contracts.

(4) Existing multiple-year task and delivery orders exceeding $100,000 awarded under IDIQ or FSS contracts, with a task/delivery order performance period of 1 year or more remaining as of January 16, 2008.

(5) New multiple-year BPA orders that exceed $100,000.

(6) Existing multiple-year BPA orders with a performance period of 1 year or more remaining as of January 16, 2008.

(7) New multiple-year contracts with option periods/quantities.

(8) Existing multiple-year contracts with option periods/quantities remaining as of January 16, 2008.

(d) Before adding funds to a multiple-year contract or order—*see 339.201–70(c)*, that involves the acquisition of EIT products and services, including EIT deliverables such as electronic documents and reports, subject to Section 508 of the Rehabilitation Act of 1973, as amended, the Contracting Officer shall ensure that the contractor has provided to the Contracting Officer and COTR a properly completed HHS Section 508 Annual Report—*see* Section 508 policy on HHS Office on Disability Web site. The Contracting Officer shall request that the contractor provide the report in sufficient time for its review and approval by the Contracting Officer, COTR, and the Section 508 Official

or designee, prior to funding performance beyond the currently funded contract performance period. The Contracting Officer shall ensure that the report and all related approvals are made a part of the official contract/order file. The Section 508 Official or designee shall monitor the Annual Reports, direct corrective measures to improve their submission and quality, and report improvement actions taken to the HHS Office on Disability.

339.203 Approval of exceptions.

(a) Procedures to document exception and determination requests are set forth in the OPDIV/STAFFDIV Section 508 Implementation Plans required by paragraph 4.1 of the HHS Section 508 policy.

(b) In the development of an AP or other acquisition request document, the Contracting Officer shall ensure that all Section 508 commercial nonavailability or undue burden exception determination requests for applicable EIT requirements are: (1) Documented and certified in accordance with the requirements of paragraph 4.3, Section 508 Compliance Exceptions, of the HHS Section 508 policy; (2) signed by the Project Officer; (3) approved by the OPDIV Section 508 Official or designee; and (4) included in the AP or other acquisition request document provided by the Project Officer to the contracting office.

(c) In instances where a technical evaluation has been performed, and no organization's proposed products or services meet some or all of Section 508 accessibility standards, in order to proceed with the acquisition, the Contracting Officer shall provide an exception determination request along with the technical evaluation panel's assessment of the Section 508 evaluation factor to the designated Section 508 Official or designee for review and approval/disapproval. *See 315.304* regarding obtaining approval of technical evaluation panel assessments by the Section 508 Official or designee. The Contracting Officer shall include the Section 508 Official's or designee's approval/disapproval of the exception determination request in the official contract file and reference it, as appropriate, in all source selection documents. For further information, *see* paragraphs 4.3, Section 508 Compliance Exceptions, and paragraph 11, Appendix A, of HHS Section 508 policy—*see* Section 508 policy on HHS Office on Disability Web site.

Subpart 339.70—Use of General Services Administration Blanket Purchase Agreements for Independent Risk Analysis Services

339.7000 Policy.

GSA has established government-wide BPAs for independent risk analysis services, including verification and validation of in-house risk assessments. For information on ordering procedures, *see* the attachment to OMB memorandum (M–08–10), Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA), dated February 4, 2008, available on the OMB Web site. HHS policy is for contracting activities to use the GSA BPA sources to the maximum practicable extent.

339.7001 Request for approval to make an award to other than a GSA BPA holder.

The Contracting Officer, in conjunction with the OPDIV/STAFFDIV Chief Information Security Officer (CISO), may determine, as part of conducting market research for independent risk analysis services expected to exceed the micro-purchase threshold, that obtaining the required services from a source other than a GSA BPA holder will result in the best value to the Government. In that event, the Contracting Officer shall prepare a request for approval at least 15 business days prior to the planned date of the contract or order award and forward it through the HCA and the OPDIV/STAFFDIV CISO for concurrence, to the SPE. The SPE shall coordinate the processing of the request with the CAO and the HHS CIO. The request for approval shall briefly describe the services required, indicate the intended source's pricing and other terms and conditions, and provide the rationale for award to the intended source rather

than the GSA BPA holders. The request may include additional supporting rationale to document the best value decision, as appropriate.

339.7002 Notice of intended award.

The CAO, or designee, in conjunction with the HHS CIO, will review the Contracting Officer's request for approval to make an award to other than a GSA BPA holder for independent risk analysis services and either approve or disapprove the request in writing. If the CAO, or designee, approves the request, upon approval, the CAO, or designee, shall send a notice of intended award to the designated GSA BPA Contracting Officer, with a copy to OMB's E-Government and Information Technology Administrator, at least 10 business days prior to the date of the proposed award explaining how it provides the best value to the Government. In the event of unusual and compelling urgency, the CAO, or designee, shall provide the notice of intended award to GSA as soon as practicable.

Subpart 339.71—Information Security Management

339.7100 Definitions.

As used in this subpart, the following definitions shall apply:

Adequate security means, in accordance with OMB Circular A–130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Federal information means, in accordance with OMB Circular A–130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Federal information system means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Information means, in accordance with OMB Circular A–130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information infrastructure means the underlying framework that information systems and assets rely on in processing, transmitting, receiving, or storing information electronically.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide—

(1) *Integrity*, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) *Confidentiality*, which means preserving authorized restrictions on access and disclosure, including means of protecting personal privacy and proprietary information;

(3) *Availability*, which means ensuring timely and reliable access to and use of information; and

(4) *Privacy*, which means regulating the appropriate collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. It essentially prohibits disclosure without consent.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

339.7101 Policy.

HHS is responsible for implementing an information security program to ensure that its information systems and associated facilities, as well as those of its contractors, provide a level of security commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the information contained in those systems. Each system's level of security shall protect the integrity, confidentiality, and availability of the information and comply with all security and privacy-related laws and regulations.

339.7102 Applicability.

Contracting Officers are responsible for ensuring that all information technology acquisitions comply with the Federal Information Security Management Act (FISMA), the HHS–OCIO Information Systems Security and Privacy Policy, and FISMA-related FAR and HHSAR requirements. This policy does not apply to national security systems as defined in FISMA.

339.7103 Solicitation and contract clause.

The Contracting Officer shall insert the clause in *352.239–72*, Security Requirements for Federal Information Technology Resources, in solicitations and contracts that involve contractor access to Federal information or Federal information systems.